

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW HAMPSHIRE**

IN THE MATTER OF THE APPLICATION OF  
THE UNITED STATES OF AMERICA FOR  
AN ORDER AUTHORIZING THE SEARCH  
OF:

No. 19-mj-134-01-AJ

ELECTRONICS SEIZED FROM JASON  
MEDLEN PURSUANT TO HIS ARREST ON  
JUNE 6, 2019

**AFFIDAVIT OF SPECIAL AGENT GALEN DOUD IN SUPPORT OF  
APPLICATION FOR SEARCH WARRANT**

I, Galen E. Doud, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been a Special Agent with the Drug Enforcement Administration (“DEA”) since May 2017, and I am currently assigned to DEA’s Manchester District Office. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am authorized to investigate violations of the laws of the United States, including violations of federal narcotics laws in Title 21 of the United States Code. While attending the DEA Training Academy, I received training on a multitude of topics pertaining to drug investigations. My primary duties as a DEA Special Agent include investigating federal crimes and violations of the Controlled Substances Act at the local, national, and international level. I have been involved in numerous drug investigations, including wiretap investigations, where I have analyzed telephone toll records and subscriber information. I have

also participated in both physical and electronic surveillances, including monitoring cell phone “pings,” the purchase of illegal drugs, enforcement operations including the execution of both search and arrest warrants, and interviews of sources of information, confidential sources, drug traffickers, and other members of drug trafficking organizations.

2. Prior to being employed as a DEA Special Agent, I was employed as a full time police officer with the City of Nashua, New Hampshire Police Department for approximately four and one-half years. I made several hundred arrests and initiated, conducted, and assisted in even more criminal investigations, many of which involved drug violations. I worked as a police officer in a uniformed and plain clothed capacity, and debriefed numerous defendants and cultivated many sources of information and confidential sources pertaining to drug trafficking organizations. I have also attended multiple trainings about drug related investigations, and relevant topics associated with drug investigations. I have a Bachelor of Science degree in Criminal Justice from Northeastern University.

3. Based on my training, education, and experience, I am familiar with the manner and means commonly employed by drug traffickers and drug trafficking organizations to conduct their illegal activities, including purchasing, manufacturing, storing, and distributing controlled substances, the laundering of illegal proceeds, and the efforts of persons involved in such activities to avoid detection by law enforcement. I am also familiar with the terminology and slang commonly employed by drug traffickers. I have observed and examined cocaine, cocaine base (“crack”), heroin, and fentanyl as well as other controlled substances. I am aware of the street prices for these substances, the methods of packaging, and the jargon used in the drug trade.

4. Based on my training and experience, I am aware that drug traffickers commonly use cellular telephones to communicate and further their drug-trafficking activities. However,

drug traffickers are aware of law enforcement's use of electronic surveillance, and thus frequently endeavor to thwart detection by changing cellular telephone numbers, using multiple cellular phones at the same time, and/or utilizing prepaid cellular phones where the user of the phone is not required to provide personal identifying information. I am also aware that drug traffickers frequently "drop" or change cellular telephone numbers and cellular telephones in an effort to thwart law enforcement's use of electronic surveillance. I am familiar with the manner in which narcotics traffickers use telephone, coded, veiled, or slang-filled telephone conversations when discussing their illegal business, in an effort to further prevent detection, and that they often use text messages in lieu of phone calls to avoid speaking over the telephone. I am familiar with the "street" language used by drug traffickers, as well as the methods they use to disguise conversation and operations.

5. As set forth in my June 7, 2019 Affidavit in Support of Application for a Complaint ("Complaint Affidavit"), attached hereto and incorporated by reference herein, I was involved in the arrest of Jason MEDLEN ("MEDLEN") on June 6, 2019. MEDLEN was arrested after he was found to be in possession of approximately 300 grams of fentanyl.

#### **PURPOSE OF AFFIDAVIT**

6. This affidavit is being submitted in support of an application for a search warrant for electronic equipment seized from MEDLEN pursuant to his arrest on June 6, 2019:

- a. A black Samsung smartphone with a black and white Nike sticker on the back, bearing what is believed to be International Mobile Equipment Identity number ("IMEI") 356823096776369,<sup>1</sup> ("Telephone #1"); and

---

<sup>1</sup> The etched IMEI on this phone is worn, and some of the numbers are difficult to decipher.

b. A black smartphone with “TLC” printed on the back (“Telephone #2”). (collectively, “the Equipment”), that are in the possession of law enforcement officials, as described in Attachment A.

7. There is probable cause to believe that the Equipment contains evidence, and instrumentalities of the crimes listed above, as described in Attachment B.

8. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other law enforcement officials and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

#### **PROBABLE CAUSE**

9. As set forth in the Complaint Affidavit, investigators conducting surveillance in Lawrence and Methuen, Massachusetts observed MEDLEN conduct what they believed to be a hand-to-hand drug transaction in Lawrence. Immediately prior to conducting the suspected drug transaction, MEDLEN was observed manipulating a cellular telephone.

10. Investigators executed a traffic stop of MEDLEN’s vehicle shortly after the suspected drug transaction, and located approximately 300 grams of fentanyl in the glove box of the vehicle. MEDLEN was placed under arrest, along with the passenger in MEDLEN’s vehicle (Louis DELVECCHIO). On June 7, 2019, the Honorable Judith G. Dein, United States Magistrate Judge, District of Massachusetts authorized a criminal complaint charging MEDLEN and DELVECCHIO with one count of possession with the intent to distribute 40 grams or more of fentanyl, in violation of 21 U.S.C. §§ 841(a)(1) and (b)(1)(B)(vi) (the “Target Offense”).

11. At the time of his arrest, investigators searched MEDLEN’s vehicle and person,

and located the Equipment in MEDLEN's vehicle. MEDLEN was read his Miranda warnings and initially waived his rights, and agreed to speak with investigators. Among other statements, MEDLEN confirmed that the Equipment belonged to him, and admitted that he had purchased the approximately 300 grams of fentanyl for \$6,000 shortly before he was stopped by investigators. MEDLEN also stated that he made similar trips to Lawrence, approximately once per week, for roughly two to three months to purchase fentanyl from the same man. Investigators seized the Equipment.

12. DELVECCHIO was also read, and then waived, his Miranda rights. DELVECCHIO stated that he travelled with MEDLEN from Maine to Lawrence, Massachusetts, and that MEDLEN was sending text messages frequently throughout the trip down.

13. Based on DELVECCHIO's statements about MEDLEN using his cellular telephone frequently on the way to Lawrence, and the observations of MEDLEN manipulating his cellular telephone immediately before the suspected drug transaction, I believe MEDLEN was using Telephone #1 and/or Telephone #2 to coordinate the drug transaction, and thus was using the Equipment to participate in and facilitate the Target Offense.

#### **LOCATION OF THE EQUIPMENT**

14. The Equipment is currently in the possession of agents from DEA Manchester District Office, as described in Attachment A.

#### **PROBABLE CAUSE TO BELIEVE THAT THE EQUIPMENT CONTAINS EVIDENCE AND INSTRUMENTALITIES OF A CRIME**

15. As established above, the investigation has demonstrated that MEDLEN used electronic equipment, including cellular telephones, to participate in and facilitate the Target Offense.

16. In addition, based on my training and experience, and information provided to me

by other agents, I am aware that individuals involved in drug trafficking frequently use computers and other electronic devices, including smartphones, to carry out, communicate about, and store records related to drugs and drug trafficking. These tasks are frequently accomplished through text messages, encrypted messages, and photographs. Based on my training and experience, I know that dealers and others involved in the drug trade frequently utilize multiple mobile phones in connection with their illegal drug activity. For example, individuals involved in drug trafficking frequently utilize one phone to communicate with drug customers and another phone to communicate with other drug-related associates (*e.g.*, suppliers, runners, organizers). Individuals involved in drug trafficking frequently change their phones and/or phone numbers, and their utilization of multiple phones can mitigate the disruption associated with these changes (for example, a dealer can change the phone used to communicate with drug suppliers or organizers while not changing the phone used to communicate with customers, or vice versa).

17. As discussed above, the Equipment is currently being stored by investigators at their facilities as described in Attachment A. From my training and experience and the training and experience of law enforcement personnel who routinely handle this equipment, I understand that it has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when it first came into the investigators' possession on June 6, 2019.

18. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B's definition of computer "hardware") can now function essentially as small computers. Both Telephone #1 and #2 are smartphones. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and

receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

19. Based on my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in mobile phones, computer hardware, computer software, and storage media.

20. Based on my training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media, in particular computers’ internal hard drives, contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

### **CONCLUSION**

21. Based on the information described above, I believe that the Equipment, as described in Attachment A, contains evidence, and instrumentalities of drug trafficking, as described in Attachment B.

I, Galen E. Doud, having signed this Affidavit under oath as to all assertions and allegations contained herein, state that its contents are true and correct to the best of my knowledge, information, and belief.

/s/ Galen E. Doud  
Galen E. Doud  
Special Agent  
Drug Enforcement Administration

Subscribed and sworn to before me,  
this 10th day of June, 2019.

Andrea K. Johnstone  
Honorable Andrea K. Johnstone  
United States Magistrate Judge  
District of New Hampshire

## **ATTACHMENT A**

### **Description of Equipment to Be Searched**

The Equipment to be searched consists of the following electronic equipment seized from MEDLEN pursuant to his arrest on June 6, 2019:

- a. A black Samsung smartphone with a black and white Nike sticker on the back, bearing what is believed to be International Mobile Equipment Identity number (“IMEI”) 356823096776369,<sup>2</sup> (“Telephone #1”); and
- b. A black smartphone with “TLC” printed on the back (“Telephone #2”).

The Equipment is located at the DEA Manchester, New Hampshire District Office, in secured storage.

---

<sup>2</sup> The etched IMEI on this phone is worn, and some of the numbers are difficult to decipher.

## **ATTACHMENT B**

### **Permissible Retrieval Techniques**

The government, and anyone whose assistance the government may require, may conduct an off-premises search of the Equipment using whatever data analysis techniques appear necessary to locate and retrieve the evidence described herein, even if those techniques render the Equipment inoperable. To the extent the Equipment is damaged beyond repair, password protected, locked or otherwise inoperable and traditional data analysis techniques will not work, the government may use a data analysis technique referred to as “chip off.” “Chip off” is a process where the BGA (Ball Grid Array or memory chip) chip is removed from the cell phone/mobile device using heat or an infrared light and the chip itself is then analyzed. This is a destructive process that will render the Equipment unusable, but it may allow for the complete collection of all data stored on the memory chip.

### **Items to Be Seized**

1. All records, in whatever form, and tangible objects that constitute evidence, or instrumentalities of 21 U.S.C. § 841(a)(1) (possession and distribution of controlled substances); between April 2019 and present, including those related to:
  - a) Records of drug trafficking activities;
  - b) lists of customers and related identifying information;
  - c) any information recording schedule, whereabouts, or travel, including calendar, e-mails, cell tower, and GPS data;
  - d) all bank records, checks, credit card bills, account information, and other financial records;

- e) the identity, location, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
  - f) text messages and instant messages.
- 2. Evidence of user attribution showing who used or owned the Equipment at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- 3. Records evidencing the use of the Internet, including:
  - a) records of Internet Protocol addresses used;
  - b) records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
  - c) As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

### **Definitions**

For the purpose of this warrant:

- A. “Equipment” means any hardware, software, storage media, and data.
- B. “Hardware” means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

### **Return of Seized Equipment**

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or instrumentalities of crime.